REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05-04-2012	Master of Military Studies Research Paper	September 2011 - April 2012

4. TITLE AND SUBTITLE
Cyberspace Operators Earning Their Wings

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Larry B. Fletcher, Jr., USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
U.S. military cyber operators must adopt an operational mindset to create information and decision superiority for friendly forces and generate military effects in the operational environment. Recognizing cyberspace's purposes to augment human intellect and control structurally complex automated systems uncovers cyberspace's value to its users. Pairing its purpose with terminology that describes the informational and physical composition of cyberspace provides cyber operators a practical representation of the domain. Finally, understanding cyberspace in its general form provides cyber operators the ability to identify the military dimensions of cyberspace. In addition to understanding cyberspace's nature, cyber operators must exhibit operational behaviors. These include the manufacture and defense of friendly cyberspace as well as the ability to attack and exploit the information resources and accompanying information technology infrastructures of adversaries.

15. SUBJECT TERMS
cyberspace; cyberspace operations; information superiority; decision superiority; information operations; military effects; operational environment; information; information assurance; Internet; information technology; computer network attack; computer network defense; computer network exploitation; cognitive effects; computational effects; information environment; computer network operations; cognitive dimension; informational dimension; physical dimension

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	31	Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass			19b. TELEPONE NUMBER (*Include area code*) (703) 784-3330 (Admin Office)

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:

Cyberspace Operators Earning Their Wings

AUTHOR:

Major Larry Fletcher, USAF

AY 11-12

Mentor and Oral Defense Committee Member: Craig A Swanson, PhD
Approved: [signature]
Date: 5 April 2012

Oral Defense Committee Member: [signature]
Approved: ADAM COSB
Date: 4/5/12

Executive Summary

Title: Cyberspace Operators Earning Their Wings

Author: Major Larry Fletcher, United States Air Force

Thesis: U.S. military cyber operators must adopt an operational mindset to create information and decision superiority for friendly forces and generate military effects in the operational environment.

Discussion: On 1 May 2010, the U.S. Air Force changed the designation of its Communications and Information Officer specialty from a support to an operations career field and renamed it Cyberspace Operations; however, the operators of 1 May 2010 demonstrated no behaviors that differed from those of the support troops of 30 April 2010. This paper describes the mindset the newly designated operators must adopt. First, properly understanding cyberspace's purpose and fundamental nature sets the foundation for cyber operators to meet military objectives through cyberspace. Recognizing cyberspace's purposes to augment human intellect and control structurally complex automated systems uncovers cyberspace's value to its users. Pairing its purpose with terminology that describes the informational and physical composition of cyberspace provides cyber operators a practical representation of the domain that reveals the military dimensions of cyberspace. Cyber operators must also exhibit behaviors that generate military effects through the cyberspace domain. The first behavior is the actual manufacture of cyberspace: Unlike the land, air, and maritime domains, cyberspace is a manmade domain. As organizations become increasingly dependent on cyberspace, potential adversaries will seek out its vulnerabilities and actual adversaries will seek to degrade the organization's ability to use cyberspace to an advantage; therefore cyber operators must defend the domain they manufacture. Finally, cyber operators must also possess the capability to attack or exploit those information resources and accompanying information technology infrastructures of their adversaries.

Conclusion: Cyberspace has the potential to provide U.S. forces a decisive military advantage across the spectrum of operations. For this reason, cyber operators must come to believe that information is ordnance and the information technologies they understand so well are the weapon systems that bring information to bear for effects in the operational environment. In order to manifest the operational capabilities DoD requires of them, U.S. military cyber operators must evolve beyond simply providing signals and administrative support for military forces and adopt an operational mindset.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

INTRODUCTION……...1

BACKGROUND: THE INFORMATION ENVIRONMENT……...2

UNDERSTANDING CYBERSPACE……5

DISTINGUISHING BEHAVIORS OF CYBER OPERATORS……..13

CONCLUSION……..19

ENDNOTES……..22

BIBLIOGRAPHY……..24

Preface

I have served in various Air Force communications-electronics capacities for the past twenty years. In that time, I have observed a growing crisis of identity among Air Force information technology professionals as we strive along with the rest of humanity to exploit the opportunities presented by the Information Age. As we transitioned from operators and maintainers of the communications systems warfighters employ for command and control of the kinetic battlefield to warriors operating in and through cyberspace, we have become fixated on "The Network." We have become distracted by the language of computer network attack, exploitation, and defense; and lost sight of the fundamental importance of information and its cognitive and computational value to people. Concurrently, we have become so fascinated with the word "cyberspace" and its association with the Internet, we tend to treat those information technology infrastructures not immediately associated with the Internet's military cousins as second class capabilities; yet these infrastructures saturate the operational environment and predominate it at the moment of crisis.

This paper contains my thoughts on the characteristics of the mindset I believe would-be cyber operators need to adopt to be effective in this new operational domain of cyberspace. We must recalibrate our understanding of the larger scope of cyberspace and reorient our focus on information and its cognitive and computational value to people. With the proper focus on the cognitive and computational value of information, information technology professionals turned cyberspace operators will realize a fitting identity and amplify their relevance in military operations.

I would like to express profound gratitude to my lovely wife, Christy. She has demonstrated an amazing amount of patience and support while I spent long hours sequestered in my study preparing this paper. Thank you for keeping me straight and focused!

I would also like to thank Lt Col John Smail, Lt Col Kevin Johnson, Major Carlos Alford, Major Bob Parker, Major Reid Novotny, and Captain Scott Ryder. The respect I have these talented Cyber Operators translated into anxiety as I exposed my ideas to them for review. As usual, each offered insightful recommendations and meaningful constructive criticism. Thank you gentlemen for not laughing too loud.

INTRODUCTION

By the stroke of a pen on 1 May 2010, the U.S. Air Force changed the designation of its Communications and Information Officer specialty from a support to an operations career field and renamed it Cyberspace Operations. Although the Air Force required each of the new cyber operators to complete a course of training to earn cyberspace operations qualification commensurate with their rank, the work and behavior of these men and women did not change appreciably between 30 April and 1 May. What change must take place in Communication and Information Officers to transform them into effective Cyberspace Operations Officers? With the U.S. military's near absolute reliance on cyberspace and many of its allies and adversaries sharing this dependence, more than a mere duty title must evolve.

The Department of Defense (DoD) is utterly dependent on electronic information and the information technology infrastructure that enables its use. DoD depends on more than 15,000 networks and seven million computing devices[1] to carryout intelligence activities, network centric operations, command and control (C2) of forces, execution of logistics functions, and management of human resources. As a result of DoD's heavy reliance on cyberspace, criminals, non-state actors, and the military and intelligence services of foreign countries constantly assail DoD electronic information and infrastructure. Nefarious actors probe DoD networks millions of times per day occasionally finding new weaknesses through which they have exfiltrated enormous amounts of information.[2] They may also exploit these weaknesses to cripple DoD's cyberspace capabilities in much the way an unidentified perpetrator tried to cripple Estonia's and Georgia's capabilities in 2007 and 2008 during disputes with Russia.[3] Although the magnitude of success for these cyber attacks may be debatable, they demonstrate that adversaries will likely employ cyberspace capabilities during conflict. For the U.S. military, this is a serious concern.

Successful comprehensive cyber attacks against military electronic information or information infrastructure could catastrophically degrade the U.S.'s ability to defeat adversaries or deter potential adversaries. Conversely, the U.S. must be able to hold its actual and potential adversaries' electronic information or information infrastructure at risk in order to obtain information superiority.

This paper will describe the characteristics of the operational mindset cyber operators must adopt to create information and decision superiority for friendly forces and generate military effects in the operational environment. First, the paper will provide a background description of the information environment and its linkage to the operations environment. Following the background, the paper will propose the manner in which cyber operators should understand cyberspace, and end with a description of the behaviors cyber operators should exhibit to distinguish themselves from information technology support specialists.

BACKGROUND: THE INFORMATION ENVIRONMENT

Information has played a key role in military operations since the beginning of organized violent conflict among humans. In the earliest days of human conflict, commanders communicated their battle plans to their warriors by some combination of visual and audial information exchange. Commanders may have employed the spoken word, the written word if literate, and visual formats that may have been as simple as drawings on a dirt floor. Once the fighting started, commanders had to control their warriors in order to adapt to the situational changes for which the plan was insufficient. Over the centuries, as the means for combat grew more sophisticated and battlefields grew too large for commanders' voices alone to control forces, warring armies began to employ audial and visual instruments like drums, bugles, and flags to communicate information on the battlefield. In modern conflicts, commanders at all

levels issue orders over vast distances in mountainous or urban terrain using radio technology. Concurrently, soldiers at the lowest echelons often have tremendous situational awareness of the larger battlefield afforded by information technologies that gave birth to the now dormant idea of Network-Centric Warfare. Advances in information technology have changed warfare's information environment throughout history.

The information environment on which military forces depend derives from the nature and character of warfare. According to Joint Publication (JP) 3-13, *Information Operations*, the information environment comprises three dimensions: cognitive, informational, and physical.[4] The cognitive dimension, the most important of the three "is the dimension in which people think, perceive, visualize, and decide."[5] In the unchanging nature of warfare, this is the dimension in which human combatants win and lose battles and wars. It is in the mind of the vanquished where they perceive their opponents have beaten them, or they decide to quit the fight before the price of war grows too great. Additionally, before and during military operations, humans make decisions about how to fight or operate in order to win. The information they have at hand aids or hinders their ability to make correct, battle-winning decisions.

Although the type of information humans judge in warfare changes with the character of warfare, warfare's nature remains unchanged in that humans require information to observe their environment and make meaningful decisions. JP 3-13 defines the informational dimensional as "where information is collected, processed, stored, disseminated, displayed, and protected. . . . It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected."[6] The informational dimensional is not a physical place despite the definition's use of "where." The informational dimension consists of information. JP 1-02, *DoD*

Dictionary of Military and Associated Terms defines information as "facts, data, or instructions in any medium or form;" or "the meaning that a human assigns to data by means of the known conventions used in their representation."[7] Information exists in the minds of humans or is stored in a physical medium residing in the physical dimension of the information environment awaiting exposure to a human or machine capable of discerning and processing it. While human's process information in the cognitive dimension, machines, lacking the capacity for cognition, process or manipulate information in the informational dimension. Concurrently, both humans and machines exist in the physical dimension.

The physical dimension is the centerpiece of the information environment. The physical dimension links humans and machines to information possessed by other humans or machines. JP 3-13 offers the following definition of the physical dimension:

> The physical dimension is composed of the command and control (C2) systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations.[8]

All methods of communication depend on the physical dimension. When humans speak to one another, the information they are transmitting transits the non-vacuous medium present between the speaker's larynx and the listener's inner ear. Even information transmitted in radio waves travelling through the vacuum of space exist in the physical dimension: Physical changes to the levels of electromagnetic energy in relation to time and a point in space represent information.

This paper will refer back to the information environment many times as it describes the characteristics of the mindset cyber operators must adopt to distinguish themselves from communications and information support specialists. The interrelationship of the cognitive, informational and physical dimensions of the information environment forms the basis for

effective cyberspace operations. Combining these dimensions appropriately will enable cyberspace operators to achieve information superiority over their adversaries contributing directly to victory on the battlefield and success in all operational environments.

UNDERSTANDING CYBERSPACE

In order to achieve military objectives through cyberspace, cyber operators must understand cyberspace's purpose and fundamental nature. Often cyber operators become fixated on "The Network" losing sight of the information needs of friendly and adversary users. Additionally, cyber operators and users mistakenly identify the Internet and its military cousins as the limits of cyberspace forgetting that the host of communications capabilities that predate the term "cyberspace" comprise important portions of the domain. Gaining an appropriate understanding of cyberspace will broaden the cyber operator's aperture and sharpen his or her sight picture. This section of the paper will make three points along these lines. First, cyber operators must acknowledge that cyberspace serves no other purposes than to augment human intellect and control structurally complex automated systems performing labor for which human intellect is unneeded or unsuited. Second, cyber operators must be able to describe cyberspace in terms relevant to its purposes. Finally, cyber operators must have the ability to identify the military dimensions of cyberspace.

Purposes of Cyberspace

As the foundation to their understanding of cyberspace, cyber operators must acknowledge that cyberspace serves no other purposes than to augment human intellect and control structurally complex automated systems performing labor for which human intellect is unneeded or unsuited. Cyber operators must view cyberspace not as a collection of electronic

hardware, but rather as an integrated virtual and physical space of human manufacture. Humans designed cyberspace to acquire, process, store, transport, control, protect, disseminate, and present information in order to generate cognitive effects among human users or computational effects in information dependent automated machines serving the purposes of human users. In an article he wrote for the book *Cyberpower and National Security*, Dr. Daniel T. Kuehl of the U.S. military's National Defense University shortens this description to three words: connectivity, content, and cognition.[9] First, *connectivity* represents the physical information technology components interconnected and configured to store, transmit, acquire, and process information. Next, *content* refers to the seemingly infinite amount of information available in cyberspace. The third item, *cognition* is the effect cyberspace has on humans once they experience access to the information cyberspace makes available. A fourth item mentioned in this paragraph's opening sentence, but to which Dr. Kuehl does not specifically refer, is distributed automation controlled by computational effect.

Humans have created interconnected automated systems that operate over vast geographic areas and require only limited human intervention to do the work humans designed them to do. Examples of where this occurs include portions of supervisory control and data acquisition (SCADA) systems for automated industrial processes, aerial bombs using the Global Positioning System (GPS) to guide themselves to target, and the underlying control processes that enable the Internet to function. The interconnected components comprising these systems largely operate without a "human in the loop" and depend on one another for data or control signals to manage system functionality. Whether this includes digital information representing the load requirements of a regional electrical power grid, or an *acknowledgement* packet in the Internet's Transmission Control Protocol, the underlying principle is similar: The machines

measure for themselves their performance and adjust or control themselves in accordance with the parameters with which their human makers designed them. To operate correctly, the information these systems exchange must be available, authentic, and protected from disclosure to unauthorized users. Whether the information an automated system receives meets these criteria or not, the information will cause a computational effect; however, if the receiving system receives correct authentic information in the format the automated system was designed to use, and the integrity of the automated system is sound, the information will cause a desired computational effect. One cannot understate the importance of accounting for information used by machines; thus cyber operators must add the idea of content for computation to Dr. Kuehl's three descriptors. *Connectivity*, *content*, *cognition*, and *computation* frame the purposes of cyberspace providing a basis for its description.

Properly Defining Cyberspace

Cyber operators must be able to describe cyberspace in relevant terms. JP 1-02 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[10] This definition is insufficient in that it focuses the reader on the physical dimension of the information environment without regard to roles of the informational and cognitive dimensions in cyberspace. In every form of its application, cyberspace's purpose is to directly serve the information needs of humans or to enable automated operation of information dependent machines human's have created to do work. Without the presence of information and its use by humans or machines, the physical components that make transmission, storage, or processing of

information possible exist only as so much physical material possessing novel electromagnetic properties.

Another shortcoming of JP 1-02's definition of cyberspace is that it encourages the reader to equate cyberspace with the Internet. Certainly, the advent of the Internet gave rise to the term *cyberspace*; however, humans have used the information technology infrastructures to which JP 1-02 refers for much longer than the terms *cyberspace* or even *information technology* have been in modern usage. Humans made their first use of cyberspace in the early nineteenth century with the advent of the railway telegraph in 1837 and Samuel Morse's subsequent invention of the magnetic telegraph in 1844.[11] By 1876, Alexander Graham Bell had invented the telephone and suddenly humans were transmitting voices and encoded text over remarkably similar information technology infrastructures built largely of copper wire.[12]

As humans found increasing usefulness for sharing information in real time over long distances, other technologies emerged that human's take for granted today. The first use of the electromagnetic spectrum for wireless transmission of textual information took place in March 1899 when Guglielmo Marconi sent a wireless telegraph message across the English Channel.[13] Soon afterward, the transmission of human speech via radio waves occurred and by 1928 the first commercial television broadcast station came to fruition.[14] As with the modern day Internet, the purpose of these technological innovations was the transmission or dissemination of information between humans or machines over long distances. Each of these technologies—wired voice and text over telegraph lines; wireless voice, video, and text in early twentieth century use of radio waves; and wireless digital audio, video, and data through today's Internet—are member elements of the larger concept humans refer to as cyberspace. Consequently, the Internet holds

no monopoly on cyberspace. To aid in clearing up the confusion of cyberspace's composition, cyber operators require a better definition of cyberspace than that offered in JP 1-02.

One can leverage the alternative definition of cyberspace that Dr. Kuehl offered in his aforementioned article:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communications technologies.[15]

Dr. Kuehl's position is that the electromagnetic spectrum may be the actual physical domain where cyber operations take place and that information-communications technologies comprise the vehicles by which humans make use of the domain.[16] In other words, information-communications technologies are to the electromagnetic spectrum as aircraft are to the earth's atmosphere, or as ships are to the maritime domain. One cannot deny the merit of Dr. Kuehl's position; however, not only does Dr. Kuehl's definition—as written—recognize the integral nature of information as a component of cyberspace, the definition's assertion that cyberspace uses electronics to perform its informational functions acknowledges the synthetic aspects of the cyberspace domain. Humans created the electronic components that make cyberspace possible specifically to store, exchange, and process information for cognitive purposes or to control machines to do work that has only limited need for the engagement of human intellect. Although Dr. Kuehl relates connectivity, context, and cognition to the definition in his writings, his definition includes no explicit mention of cognition nor distributed automation. A closer look at the purposes for which humans created cyberspace reveals that the definition remains sufficient to account for these purposes.

When considering a human's use of a desktop computer or handheld mobile computing device, the connection between humans and the information in cyberspace seems obvious;

however, when cyberspace serves as the means to control a structurally complex system like a regional electrical power grid, the connection between human and the information in cyberspace is less apparent. In the former case, the human uses cyberspace directly to obtain or share information with other humans to socialize or aid in making decisions—both of these are cognitive effects. In the latter case, humans or machines provide information to machines at a distant location to control the state of the machine—a computational effect. In this case, on the surface, the end user of the information seems to be a machine rather than a human, but the machine's purpose is to provide electrical power for human purposes such as to heat a human's home, or power a human's connection to the Internet. No matter whether the electrical power fails or operates properly, the use of cyberspace to control the power grid affects humans. The work of controlling the electrical power grid is unsuitable for humans. In portions of the electrical grid, adjustments to electrical current or voltages requires only mundane simple calculations and resulting actions that machines can do over time without suffering such human faults as complacency or fatigue. In other parts of the grid, where complexity is much higher and reactions must occur in milliseconds, only computers designed to decide and act autonomously can manage these processes effectively. In summary, in neither the cognitive nor the computational case does cyberspace exist independent of the needs of humans.

Military Dimensions of Cyberspace

The profound information-based benefits of cyberspace carry with them equally profound vulnerabilities for both private citizens and the nation-states in which they live. The developed and developing nations increasingly depend on cyberspace for social, political, economic, and military uses. Governments, businesses, and private users depend on uninterrupted and, to a large degree, confidential access to authoritative, authentic, and accurate digital information and

digital information based services. It is this dependence that creates vulnerability.[17] Both its uses and its accompanying vulnerabilities contribute to military consideration of cyberspace as an operational domain of warfare.

General Robert Kehler in his former capacity as Commander of Air Force Space Command commented that "cyberspace is about operations, not communication. It is about operations, not a network. It is about how we do things to fight and win."[18] Very little of JP 1-02's definition of cyberspace matches General Kehler's position. To realize the concept that "cyberspace is about operations," cyber operators must come to view cyberspace as the intersection of virtual and physical space they create and sustain to acquire, process, store, transport, control, protect, disseminate, and present information in order to generate cognitive effects among human users or computational effects in information dependent automated systems. Furthermore, cyber operators must see beyond the Internet and Internet-like military networks when visualizing cyberspace.

Without question, the US military is heavily dependent on its connections with the Internet through its Non-Secure Internet Protocol Router Network (NIPRNET); however, military use of cyberspace is broader than this interconnection. Many of DoD's critical C2 and intelligence systems make use of networks that are physically or cryptographically isolated from the NIPRNET and the Internet yet make use of cyberspace. The Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS) are examples with which the reader may be familiar. Both of these networks resemble the Internet, so comprehending that these networks are portions of cyberspace is no great leap; however, categorizing some of the information and information infrastructures on which many U.S. military weapon systems depend as making up a portion of cyberspace is less obvious.

Although the term Network-Centric Warfare (NCW) has fallen out of favor as a result of former Secretary of Defense Donald Rumsfeld's oft purported failed plans for U.S. military transformation, the U.S. military has come to depend on the cyberspace-enabled technologies once associated with NCW. The Enhanced Position Location Reporting System (EPLRS) and the Situation Awareness Data Link (SADL) are examples of NCW capabilities that create cyberspace of great advantage to U.S. warfighters. Ground forces may employ EPLRS to create geospatial situational awareness among friendly forces and to share information immediately increasing lethality and decreasing the likelihood of fratricide. Extending this network vertically with SADL enables friendly airpower to benefit and contribute to the information EPLRs makes available again magnifying lethality and reducing chances for fratricide. Although less intuitive than SIPRNET's belonging to cyberspace, EPLRS, SADL, and many other information systems also comprise portions of cyberspace.

Cyberspace Understood: A Summary

Properly understanding cyberspace's purpose and fundamental nature sets the foundation for cyber operators to meet military objectives through cyberspace. Recognizing cyberspace's purposes to augment human intellect and control structurally complex automated systems uncovers cyberspace's value to its users. Pairing its purpose with operationally relevant terminology that describes the informational and physical composition of cyberspace provides cyber operators a practical representation of the domain. Finally, understanding cyberspace in its general form provides cyber operators the ability to identify the military dimensions of cyberspace. This robust understanding of cyberspace hints at the behaviors cyber operators must exhibit to produce operational effects through cyberspace as this paper will explore in the following section.

DISTINGUISHING BEHAVIORS OF CYBER OPERATORS

In order to distinguish themselves from the communications and information support professionals from whence the services derived them, cyber operators must not only understand cyberspace, but must also exhibit behaviors that generate military effects through the cyberspace domain. Lieutenant General William Lord, the United States Air Force Chief Information Officer explains why the need for the distinction in an interview he gave to *Defense System Magazine*:

> When you only need to interrupt the transmission of an ISR sensor that's flying over an area of responsibility but is being analyzed tens of thousands of miles away, you don't have to go to the [hardened] target at either end . . . maybe you go to the soft target that is between. So the realization that that capability [the ten thousand mile long communication link] is more than just an enabling or a support activity but is in fact integral to the warfighting activity is what has caused us to begin to think about the communications electronic supporting activities and cyber activities in more operational terms versus more support terms. And so that creates the need for an operational mindset in people that heretofore have been in a support mindset. Not one right and one wrong, just two different mindsets.[19]

In short, the uses of cyberspace in the modern operations environment drive the need for an operational mindset among military information technologists turned cyberspace operators. This section will offer the observable behaviors operations minded cyber operators must exhibit. The first behaviors the section will describe are the manufacture and sustainment of cyberspace. Following manufacture, the section will include a description of cyber defense behaviors. Finally, the section will briefly address cyber attack and exploitation.

Manufacturing Cyberspace

Recall that unlike the land, air, and maritime domains, cyberspace is a manmade domain; therefore, cyberspace operators must possess the technical capacity to establish, configure and sustain an information technology infrastructure capable of fulfilling the functions of the military communications system: acquire, process, store, transport, control, protect, disseminate, and

present information.[20] While remembering these functions are important, retaining the traditional mindset is unsatisfactory. Cyber operators who understand Information Operations (IO) can employ the communications system functions operationally by reordering the sequence of the IO process, and reversing the purposes of some IO activities. In January 2011, the Secretary of Defense, Dr. Robert Gates defined IO as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[21] Joint Publication (JP) 3-13, amplifies the description of IO stating that "a key goal of IO is to achieve and maintain information superiority for the US and its allies. Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior decisions."[22] Cyber operators should seize upon the IO concept that the purpose of information-related capabilities is to affect decision making capabilities of adversaries or produce superior decisions by friendly forces. When one considers that computer network operations (CNO) comprise one of the core information-related capabilities to which Secretary Gates referred in his new definition of IO, this does not seem to be too great a step. The trick is to convince cyber operators to think in terms of information and resulting decisions rather than focusing first on the hardware, software, and firmware of information technology.

The cyber operator—who must achieve decision superiority for friendly forces by establishing, configuring and sustaining an information technology infrastructure—should employ an inverse of the IO process as illustrated in the following text. Where information operators select their target audiences from among actual or potential adversaries, the Joint Force Commander assigns cyber operators their target audiences from among friendly forces. Next,

where information operators determine the cognitive effects they need to induce in their target audiences, friendly target audiences identify to cyber operators the cognitive or computational effects they need to experience. In the final step, both information operators and cyber operators determine the best source for the information their respective audiences need, establish or identify the information infrastructure required to make the information available, and entice their audiences to make use of the infrastructure.

Defending Cyberspace

After the ability to establish functioning information technology infrastructure, the next most important attribute a cyber operator must have is the ability to defend the infrastructure and the electronic information residing therein from attack and other threats. Cyber operators refer to this capability as information assurance (IA). JP 3-13, *Information Operations* defines IA "as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[23] In other words, cyber defenses serve to ensure the availability of information resources for information users; maintain the confidentiality of information by preventing its disclosure to those who are not authorized to access it; and to protect the integrity of information by attributing authorized changes to it or preventing unauthorized changes. To accomplish these tasks, cyber operators employ a combination of proactive or reactive defenses to which they should collectively refer as information assurance.

Proactive defenses begin in the design phase of creating information technology infrastructure. These defenses include among other things robust electrical design, secure software design, environmental control, physical security, and personnel security applied to both

information users and cyber operations staff. Other proactive defenses may include cryptography, logical firewalls within the virtual portion of cyberspace, fire suppression systems within the physical portion of cyberspace, and a system to achieve cyberspace user authentication and non-repudiation. Proactive defenses are measures cyber operators put in place to reduce known vulnerabilities and counter known threats to electronic information and the infrastructure on which it depends.

Cyber operators employ reactive defenses to address unknown threats and vulnerabilities and those known vulnerabilities that generate risks cyberspace users must accept to benefit from cyberspace capabilities. Risk is a function of threat and vulnerability and sometimes expressed in terms of risk equaling the mathematical product of threats and vulnerabilities. Using this mathematical model (i.e., Risk = Threat x Vulnerability)[24] one can appreciate that if either threats or vulnerabilities are reduced to zero, risk becomes zero, too. Unfortunately, cyber operators may reduce vulnerabilities but can never eliminate them all. Concurrently, threats will likely never disappear; so, in the end, some risk associated with the use of cyberspace will always remain. While proactive defenses attempt to reduce risk to manageable and acceptable levels, reactive defenses exist to deal with the ever evolving residual risk. An example of reactive defense is the use of an intrusion detection system to cue cyber operators to the need for action or an intrusion prevention system that responds to perceived intrusions with automatic responses.

Another component of IA is planning for continuity of operations in face of attack or other disastrous situations. Effective IA planning will have in place alternate infrastructures to assume the information workload for critical information systems, or some degree of information

technology resources set aside to reconstitute damaged infrastructure and information resources. Closely related to IA is the Air Force's concept of mission assurance.

Perhaps the single most distinguishing characteristic of cyber operators is their grasp of the concept of mission assurance. Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations* states that mission assurance "entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities."[25] At first glance, mission assurance appears to be not much more than IA's reactive defense; however, mission assurance varies significantly. Whereas IA is an overarching principle that cyber operators seek to employ throughout the breadth and depth of their information technology infrastructures, the number of vulnerabilities outstrip the resources cyber operators may bring to bear to mitigate them all at once. Mission assurance differs in that it brings significant defensive resources to bear on known vulnerabilities for a specified period determined by the length and importance of discreet missions, and then frees those resources for other missions as operational needs dictate.

Attacking and Exploiting Cyberspace

Cyber operators must also possess the capability to attack or exploit those information resources and accompanying information technology infrastructures of their adversaries. For many of the same reasons friendly forces employ cyberspace, adversaries are also likely to seek to leverage information technology for military, economic, or diplomatic advantage. Possessing the ability to degrade an adversary's information resources while strengthening and protecting one's own may prove decisive in conflict.

Cyber operators working independently or as a component of a larger IO plan may employ computer network attack (CNA) to deceive, degrade, disrupt, and deny adversary

electronic information and infrastructure.[26] Just as with any IO function, the cyber operator must understand his commander's intent, formulate the appropriate effects he must have in the mind of his adversary—a cognitive effect—determine the information that he must disrupt or corrupt to achieve his desired effects, and, finally, choose the information infrastructure he will attack to disrupt or corrupt the targeted information. Successful CNA improves the decision capabilities of friendly forces when considered in relation to decision capabilities existing before the attack.

Cyber operators must also possess the capability to perform reconnaissance and surveillance of an adversary's information technology infrastructure and the information residing there in. By learning the technical details of an adversary's information technology infrastructure, one may detect its vulnerabilities in preparation for attack of the infrastructure or the resident information. One may also exploit these vulnerabilities simply to gain access to the information an adversary stores or exchanges via his or her information technology infrastructure for its intelligence value in relation to the various aspects of conflict.

Summary of Behaviors

Cyber operators must exhibit behaviors that generate military effects through the cyberspace domain. The first behavior is the actual manufacture of cyberspace: Unlike the land, air, and maritime domains, cyberspace is a manmade domain. As organizations become increasingly dependent on cyberspace, potential adversaries will seek out its vulnerabilities and actual adversaries will seek to degrade the organization's ability to use cyberspace to an advantage; therefore cyber operators must defend the domain they manufacture. Finally, cyber operators must also possess the capability to attack or exploit those information resources and accompanying information technology infrastructures of their adversaries.

CONCLUSION

U.S. military cyber operators must adopt an operational mindset to create information and decision superiority for friendly forces and generate military effects in the operational environment. Cyberspace has the potential to provide U.S. forces a decisive military advantage across the spectrum of operations. For this reason, cyber operators must come to believe that information is ordnance and the information technologies they understand so well are the weapon systems that bring information to bear for effects in the operational environment. In order to manifest the operational capabilities DoD requires of them, U.S. military cyber operators must evolve beyond simply providing signals and administrative support for military forces and adopt an operational mindset.

Understanding Cyberspace and Operating in the Domain

Properly understanding cyberspace's purpose and fundamental nature sets the foundation for cyber operators to meet military objectives through cyberspace. Recognizing cyberspace's purposes to augment human intellect and control structurally complex automated systems uncovers cyberspace's value to its users. Pairing its purpose with terminology that describes the informational and physical composition of cyberspace provides cyber operators a practical representation of the domain. Finally, understanding cyberspace in its general form provides cyber operators the ability to identify the military dimensions of cyberspace. This robust understanding of cyberspace hints at the behaviors cyber operators must exhibit to produce operational effects through cyberspace.

Cyber operators must exhibit behaviors that generate military effects through the cyberspace domain. The first behavior is the actual manufacture of cyberspace: Unlike the land, air, and maritime domains, cyberspace is a manmade domain. As organizations become

increasingly dependent on cyberspace, potential adversaries will seek out its vulnerabilities and actual adversaries will seek to degrade the organization's ability to use cyberspace to an advantage; therefore cyber operators must defend the domain they manufacture. Finally, cyber operators must also possess the capability to attack or exploit the information resources and accompanying information technology infrastructures of their adversaries.

Information Technology's Legacy

Despite the modern interest surrounding the operation, attack, and defense of cyberspace, some may argue nothing is new regarding human use of information technology other than rhetoric. After all, as in the Air Force example, the Cyberspace Operators of 1 May 2010 demonstrated no behaviors that differed from those of the Communication and Information Officers of 30 April 2010. Additionally, cyberspace operators' technical capacity to manufacture information technology infrastructures capable of acquiring, processing, storing, transporting, controlling, protecting, disseminating, and presenting information seems to be nothing more than building the military communications system that existed prior to modern use of the word "cyberspace." Finally, many may question the need for a definition of cyberspace that differs from that offered in JP 1-02. In short, those who follow these lines of thought might argue that the status quo is sufficient.

Recommendations

The services must continue efforts to overcome the mental inertia that may inhibit the realization of an operational mindset among their cyber professionals. The services must indoctrinate both their cyber operators and the users of cyberspace regarding the nature and importance of an operational mindset. As with any useful military behavior, indoctrination should begin early in the careers of operators and users. For cyber operators, the amount of

training required to manufacture, operate, defend, attack, and exploit cyberspace in all its forms is enormous requiring a graduated training regimen that should span a career.

In order to keep sight of the purposes of cyberspace, cyber operator training should include a mid-career requirement to gain qualification in information operations. Information operations demand that the operator understand the affect of information on the human mind. Learning to integrate the information-related capabilities to influence, disrupt, corrupt, or usurp the decision-making of actual and potential adversaries while protecting one's own[27] provides a springboard framework for commanding a comprehensive cyberspace campaign. Such a campaign would weave together the cyberspace manufacture, attack, and defend behaviors throughout the operational environment to generate effects for friendly forces and on adversaries at the tactical, operational, and strategic levels of warfare.

Endnotes

[1] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (July 2011), http://www.defense.gov/news/d20110714cyber.pdf, 1 (accessed August 26, 2011).

[2] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (July 2011), http://www.defense.gov/news/d20110714cyber.pdf, 3 (accessed August 26, 2011).

[3] Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," *Defense Horizons* 68 (September 2009), http://www.ndu.edu/CTNSP/index.cfm?secID=16&pageID=4&type=section, 3 (accessed December 12, 2011).

[4] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-1.

[5] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-2.

[6] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-2.

[7] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02, As Amended through October 15, 2011 (Washington, DC: Joint Chiefs of Staff, November 8, 2010), 164.

[8] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-1.

[9] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, ed. D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28.

[10] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02, As Amended through October 15, 2011 (Washington, DC: Joint Chiefs of Staff, November 8, 2010), 86.

[11] Sir Eric Eastwood, "telegraph," *Academic American Encyclopedia*, vol. 19 (Danbury, CT: Grolier Incorporated, 1991), 76 - 77.

[12] Sir Eric Eastwood, "telegraph," *Academic American Encyclopedia*, vol. 19 (Danbury, CT: Grolier Incorporated, 1991), 76 - 77.

[13] Allen Mottershead, "radio," *Academic American Encyclopedia*, vol. 16 (Danbury, CT: Grolier Incorporated, 1991), 44.

[14] Federal Communications Commission, "Visionary Period, 1880's Through 1920's," *Historical Periods in Television Technology*, http://transition.fcc.gov/omd/history/tv/1880-1929.html (accessed January 10, 2012).

[15] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, ed. D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28.

[16] Daniel T. Kuehl, "CYBERSPACE: Its Place in National Security"‖ (lecture, Marine Corps University, Quantico, VA, January 27, 2012).

[17] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, ed. D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28.

[18] Air Force Space Command, *Air Force Space Command Functional Concept for Cyberspace Operations* (2010), https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1344B60FB5E044080020E329A9/Files/editorial/Functional%20Concept%20for%20Cyberspace%20Ops%20%20(Final--14%20Jun%202010).pdf?channelPageId=s6925EC1344B60FB5E044080020E329A9&programId=t6925EC2AD3920FB5E044080020E329A91, 1 (accessed August 26, 2011) .

[19] Barry Rosenberg, "Air Force CIO Pushes for Operational Mindset," *Defense Systems*, August 11, 2009, http://defensesystems.com/articles/2011/08/08/interview-lt-gen-william-lord.aspx?sc_lang=en (accessed December 18, 2011)

[20] Joint Chiefs of Staff, *Joint Communications System*, JP 6-0 (Washington, DC: Joint Chiefs of Staff, June 10, 2010), I-7.

[21] Secretary of Defense Memorandum for the Secretaries for the Military Departments, *Strategic Communications and Information Operations in the DOD* (Washington, DC: Office of the Secretary of Defense, January, 25, 2011).

[22] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-1.

[23] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), II-5.

[24] Shon Harris, *CISSP Exam Guide*, 5th ed. (New York, NY: McGraw Hill, 2009), 100.

[25] United States Air Force, *Cyberspace Operation*, AFDD 3-12, (July 15, 2010), www.e-publishing.af.mil, 7 (accessed December 13, 2011).

[26] Joint Chiefs of Staff, *Information Operations*, JP 3-13 (Washington, DC: Joint Chiefs of Staff, February 13, 2006), II-5.

[27] Secretary of Defense Memorandum for the Secretaries for the Military Departments, *Strategic Communications and Information Operations in the DOD* (Washington, DC: Office of the Secretary of Defense, January, 25, 2011).

Bibliography

Air Force Space Command. *Air Force Space Command Functional Concept for Cyberspace Operations*, 2010. https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1344B60FB5E044080020E329A9/Files/editorial/Functional%20Concept%20for%20Cyberspace%20Ops%20%20(Final--14%20Jun%202010).pdf?channelPageId=s6925EC1344B60FB5E044080020E329A9&programId=t6925EC2AD3920FB5E044080020E329A91 (accessed August 26, 2011) .

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* July 2011. http://www.defense.gov/news/d20110714cyber.pdf (accessed August 26, 2011).

Eastwood, Sir Eric. "telegraph." Vol. 19. *Academic American Encyclopedia*. Danbury, CT: Grolier Incorporated, 1991.

Federal Communications Commission, "Visionary Period, 1880's Through 1920's," *Historical Periods in Television Technology*, http://transition.fcc.gov/omd/history/tv/1880-1929.html (accessed January 10, 2012).

Harris, Shon. *CISSP Exam Guide*. 5th ed. New York, NY: McGraw Hill, 2009.

Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. JP 1-02, As Amended through October 15, 2011. Washington, DC: Joint Chiefs of Staff, November 8, 2010.

Joint Chiefs of Staff. *Information Operations.* JP 3-13. Washington, DC: Joint Chiefs of Staff, February 13, 2006.

Joint Chiefs of Staff. *Joint Communications System*. JP 6-0. Washington, DC: Joint Chiefs of Staff, June 10, 2010.

Kuehl, Daniel T. "CYBERSPACE: Its Place in National Security." Cyber lecture, Seminar 4: National Strategy, Marine Corps University, Quantico, VA, January 27, 2012.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." *Cyberpower and National Security*, Edited by D. Kramer, Stuart H. Starr and Larry K. Wentz. Washington, DC: National Defense University Press, 2009, 3-42.

Miller, Robert A. and Kuehl, Daniel T. "Cyberspace and the 'First Battle' in 21st-century War." *Defense Horizons* 68,fs September 2009. http://www.ndu.edu/CTNSP/index.cfm?secID=16&pageID=4&type=section, 3 (accessed December 12, 2011).

Mottershead, Allen. "radio," Vol. 16. *Academic American Encyclopedia*. Danbury, CT: Grolier Incorporated, 1991.

Rosenberg, Barry. "Air Force CIO Pushes for Operational Mindset." *Defense Systems*, August 11, 2009. http://defensesystems.com/articles/2011/08/08/interview-lt-gen-william-lord.aspx?sc_lang=en (accessed December 18, 2011)

Secretary of Defense Memorandum for the Secretaries for the Military Departments. *Strategic Communications and Information Operations in the DOD*. Washington, DC: Office of the Secretary of Defense, January, 25, 2011.

United States Air Force. *Cyberspace Operation*. AFDD 3-12. July 15, 2010. http://www.e-publishing.af.mil (accessed December 13, 2011.